DETAILED INSPECTION CHECKLIST

FA SC STMT	TEXT
405	INFORMATION SYSTEMS MGMT Functional Area Manager: HQMC C4/Cybersecurity Point of Contact: MGySgt Leroy Hall and Diane Clarke Email: leroy.hall@usmc.mil; diane.clarke@usmc.mil (DSN) 233-3490 (COML) 703-693-3490 Date Last Revised: 23 October 2014
405 01	ADMINISTRATIVE, POLICIES AND STANDARDS
405 01 001	Does the command G6/S6 have a current Table of Organization and Equipment (T/O&E) on hand and does it contain the unit mission statement if command has its own UIC in MCTFS and has it been reviewed and updated every four years as per the order? Reference MCO 5311.1D; MCO P4790.2C
405 01 002	Does the command G6/S6 have suitable turnover folders/desk-top procedures containing the required information necessary to run routine daily operations? Reference MCO P4790.2C
405 01 003	Does the command fully comply with DoD policy mandating due diligence (need-to- know and background security checks) and use of System Authorization Access Request form (SAAR, DD2875, USMC version) before granting access to all DoD/USMC Information Systems? Reference CJCSI 6510.01F; SECNAV 5239.3B; MCO 5239.2A
405 01 004	Are all command Information Systems (IS) in compliance with DoD policy mandating the use of the “Standard Mandatory DoD Notice and Consent Reference CJCSI.6510.01F; MARADMIN 692/08
405 01 005	Are classification labeling, designation, or markings clearly and properly identified by physical, electronic, or other means for each classified media (documents, computers, external hard drives, etc.)? Reference EO 13526; DoD 5200.01, Volume 2; SECNAV M-5510.30; SECNAV M-5510.36
405 01 006	Are all audit records (events, OS, application-specific logs) properly managed, maintained, and protected from breaches of confidentiality and integrity? Reference CJCSI 6510.01F; DODI 8500.01; SECNAV M-5239.1

405 01 007 Are periodic Fire Marshall Inspections (annually at a minimum) of computing facilities including server rooms being properly conducted and tracked?
References :
DoDI 6055.06; DoD IG Report No. D-2008-138Report No. D-2008-138

405 01 008 Does the command have a written policy regarding the use of personal resources, privately owned or leased personal computers (to include contractor owned computers) for conducting both official or unofficial business in a government workplace?
Reference
CJCSI 6510.01F; ECSD 014; ECSD 005; MARADMIN 375/01

405 01 009 Are passwords/authentication methods transmitted through unsecure transmission modes or stored in clear text/plain text (i.e. telnet, FTP, TFTP, SNMPv1, SNMPv2, PAP, POP3, BSD [rexec, rcp, rsh, rlogin, rdist, etc…], IGRP [RIPv2, EIGRP, OSPFv2, IS-IS], and database my SQL, Oracle, db odbc)?
Reference
NETWORK INFRASTRUCTURE STIG V7R1, par 5.3, STIG ID NET1638; GENERAL DATABASE SECURITY CHECKLIST V8R1.4; ECSD 004

405 01 010 Are all IT assets, and user accounts properly managed with established policy and procedures for monitoring all user account inactivity, to include privileged users?
Reference
DODI 8500.2; SECNAV M-5239.1

405 02 C AND A/RISK MANAGEMENT FRAMEWORK/PPSM REQUIREMENTS

405 02 001 Are all DoD IS's up-to-date on accreditation decisions (ATO, IATO, IATT or DATO)?
Reference
CJCSI 6510.01F; DoDI 8510.01; ECSD 018

405 02 002 Are all IA roles (CAR, Validator, Analyst, IAM, IAO, ISSM, ISSO, etc.) identified and appointed in writing by the appropriate authority and does the appointment letter include a statement of IA responsibilities?
Reference
DODD 8500.01; DoDI 8510.01; SECNAV M-5239.1; MCO 5239.2A; ECSD 018

405 02 003 Is the IA posture, situational awareness, and C&A related documentation (IT Security POA&M, DIP, SIP, and FISMA related reporting requirements) being properly maintained in MCCAST?
Reference
DoDI 8510.01; DoD 8530.01-M; SECNAV M-5239.1; ECSD 018

405 02 004 If commercial wireless networks are in use, have they been approved by the local spectrum manager and the Marine Corps DAA through the MCEN C&A process?
Reference
SECNAV 5239.3B; SECNAV 2075.1; ECSD 014

405 02 005 Has the risk management process been properly employed to include the Mission Assurance Category (MAC) of the system, the classification or sensitivity of information handled by the system, potential threats, documented vulnerabilities protection measures, need-to-know, and survivability enhancements in transmission paths, routing, equipment, and associated facilities?
Reference
DoDD 8510.01; DoDD 3020.26; SECNAV 5239.3B

405 02 006 Have all command Information Assurance Manager (IAM)/ Information System Security Manager (ISSM) and or current system owners obtained the required DoD PPS Registry account?
Reference
DODI 8551.1; ECSD 021; MARADMIN 371/13

405 02 007 Are all approved systems used by the command on the MCEN-N and MCEN-S fully in compliance with ECSD 021 and registered in the DoD Ports, Protocols and Services Management registry?
Reference
DODI 8551.1; ECSD 021; MARADMIN 371/13

405 02 008 Has the command G6/S6 ensured that the Marine Corps Commercial Internet Service Provider (C-ISP) waiver process has been fully implemented for all C-ISP within their purview?
Reference
CJCSI 6211.02D; DODI 8510.01; MCO 2100.7; WAN ECSD 018

405 03 TRAINING/CYBERSECURITY WORKFORCE

405 03 001 Have all command personnel taken the required initial/annual PII training?
Reference
CJCSI 6510.1F; SECNAV 5211.5E; MCO 5239.2A; MARADMIN 257/12; MARADMIN 288/13; MARADMIN 690/13

405 03 002 Have all command personnel that have a NIPRNET and SIPRNET account taken the required DoD Cybersecurity awareness training?
Reference
CJCSI 6510.1F; MCO 5239.2A; MARADMIN 257/12; MARADMIN 288/13; MARADMIN 690/13

405 03 003	Are all MCEN users using MarineNET and or Total Workforce Management Services (TWMS) to take both Cybersecurity Awareness and PII trainings annually to allow HQMC C4 to obtain accurate FISMA reporting training numbers within the Marine Corps as required by the order? Reference MARADMIN 257/12; MARADMIN 288/13; MARADMIN 690/13
405 03 004	Have all SIPRNET users taken the required initial Derivative Classification training before accounts were granted and refresher training every two years? Reference Executive Order 13526; SECNAV M-5510.36
405 03 005	Are all persons cleared for access to classified information or assigned to duties requiring a trustworthiness determination given an initial security briefing and annual security training for personnel having access to classified information? Reference SECT 271 ET SEQ. OF TITLE 15, U.S.C., "COMPUTER SECURITY ACT OF 1987"; EO 13526; DOD 5200.2-R,
405 03 006	Are all personnel performing IA privileged user or management functions, regardless of job series or military specialty and inclusive of contractors and foreign nationals, appropriately identified, documented, tracked using Marine Corps Training and Information Management System (MCTIMS) and certified according to their IAM/IAT level and if not, have the appropriate waivers been granted by the Marine Corps AO/DAA and SIAO and on file? Reference DoDD 8500.01; DoDD 8570.01; DoD 8570.01-M; SECNAV M-5239.1; ECSD 024; MARADMIN 722/10
405 03 007	Per the CMC White Letter (Information Protection), has the command developed a plan/strategy to ensure all cybersecurity personnel can obtain the required certification mandated by the DoDI 8570.01-M especially for unsupervised Privileged User? condition of access? Reference CMC White Letter (NO 1.11 INFORMATION PROTECTION); ECSD 024
405 03 008	Have all personnel performing cybersecurity functions with privileged access to any information system completed the Privileged Access Agreement form as a condition of access? Reference DoDD 8570.01; DOD 8570.01-M; SECNAV M-5239.2; MCO 5239.2A; ECSD 024

405 04 PHYSICAL/OPERATIONAL SECURITY/HARD DRIVE POLICY

405 04 001 Are all physical access points to facilities containing networks and workstations that process or display classified information guarded and/or alarmed 24x7 with specific response times appropriate to the classification of the materials protected?
Reference
DoD 5200.01, Volume 3; SECNAV M-5510.36; MCO 5530.14A

405 04 002 Are the required two-factor authentication and classified access logs maintained at the facilities containing classified information?
Reference
DoD 5200.01, Volume 3; SECNAV M-5239.1; SECNAV 5239.3B

405 04 003 Is there an established policy and program to identify (authenticate) and control visitors in restricted or controlled areas?
Reference
DoD 5200.01, Volume 3; SECNAV M-5239.1; SECNAV 5239.3B

405 04 004 Does the command have appropriate disposal of hard drives and storage media procedures and process (Computer disposal process formerly DRMO) in conjunction with regional MAGTF IT Support Center (MITSC)?
Reference
SECNAV 5510.36; MCO 4500.11E; ECSD 011

405 04 005 Does the command policy ensure all DOD/USMC magnetic hard drive storage media which are classified or non-DATA AT REST compliant, remain in proper custody control until degaussed and physically destroyed or until shipped to National Security Agency (NSA)?
Reference
DOD 5200.01 Volume 3; SECNAV 5510.36; DON CIO MSGID, PROCESSING OF ELECTRONIC STORAGE MEDIA FOR DISPOSAL, DTG 281759Z AUG 2012; MCO 4500.11E; ECSD 011

405 04 006 Does the command policy ensure proper accountability of all hard drives and securely maintain a proper record on each hard drive?
Reference
DOD 5200.01 Volume 3; SECNAV 5510.36; DON CIO MSGID, PROCESSING OF MAGNETIC HARD DRIVE STORAGE MEDIA FOR DISPOSAL, DTG 281759Z AUG 2012; ECSD 011

405 04 007 Does the command have a cyber-spillage policy containing accountability and responsibilities requirements and is this policy part of the unit training per the CMC White Letter?
Reference
CMC WHITE LETTER NO. 2-1, CYBER AWARENESS AND

ACCOUNTABILITY; ECSD 010

401 04 008 Has the command G6 established and implemented a policy directing all personnel to cease Data transfer to removal media on the SIPRNET without the proper approval?
Reference
USCYBERCOM CTO 10-133; MARADMIN 226/11

405 05 PII/IDENTITY MANAGEMENT

405 05 001 Are ISSM responsibilities for Personally Identifiable Information (PII) properly executed to include any PII incident reporting and notification procedures properly being executed?
Reference
SECNAV M-5239.1; ECSD 011

405 05 002 Are documents containing PII properly marked “For Official Use Only” or with the approved DoD PII cover sheet (DD 2923, Privacy Act Cover Sheet)?
Reference
SECNAV 5211.5E; ECSD 011; MARADMIN 389/07

405 05 003 Are publicly accessed websites managed to ensure they do not contain PII? Are any internal (private) Marine Corps websites providing access to or containing PII secured with encryption and authentication mechanisms while also limited to only those individuals with a need to know?
Reference
DoDD 8500.01; DoDI 8520.2; SECNAV 5211.5E

405 05 004 Does the command enforce the policy requiring all emails transmitting PII be digitally signed and encrypted using DoD PKI certificates and do they contain the appropriate statement notifying the recipient(s) that any misuse or unauthorized access may result in civil and criminal penalties?
Reference
OMB M-07-16 ATTACHMENT 1; DoD 5400.11-R; DoDI 8520.2; SECNAVINST 5511.5E; ECSD 011

405 05 005 Do all authorized PED, removable storage device/media users ensure that PII processed or stored PII on the device is encrypted with FIPS140-2 Level II or higher?
Reference
CJCSI 6510.01F; DoDD 8100.02; DoD 5400.11-R; DoDI 8420.01; DON CIO MESSAGE: DTG: 091256Z OCT 07; ECSD 011

405 05 006	Are proper disposal requirements for PII implemented for physical and electronic formats through procedures and internal access controls that ensure the proper disposal procedures are being followed? Reference NIST SP 800-88, par 2.1; DoD 5400.11-R; SECNAV 5211.5E; ECSD 011; MARADMIN 162/10
405 05 007	Are Privacy Impact Assessments (PIA) conducted for all relevant IT systems to include, but not limited to, locally created systems such as databases, local websites, and limited use applications at the command? Reference DOD 5400.11-R; DODI 5400.16; ECSD 011
405 05 008	Has every organizational level followed the procedures required in the SSN Reduction Plan? Reference OMB M-07-16; DODI 1000.30; SECNAV 5211.5E; ECSD 011
405 05 009	Are all IS's, including networks, e-mail, and Web servers, using PKI certificates issued by the Department of Defense and approved external PKI certificates, as appropriate, to support authentication, access control, confidentiality data integrity, and non-repudiation? Reference DODI 8520.2; SECNAV 5239.3B; MCO 5239.2A; ECSD 011
405 06	INCIDENT RESPONSE/VULNERABILITY MANAGEMENT
405 06 001	Does an incident response plan exist in writing that defines reportable incidents, outlines a standard operating procedure for incident response, provides for user training, and establishes an incident response team? Reference DOD 5200.1-R; SECNAV M-5239.1; SECNAV 3501.1C, ECSD 001
405 06 002	Are Computer Network Directives (CTO's, FragO's, OpDir's, etc…) adhered to and tracked to ensure compliance of system vulnerabilities? Reference SECNAV M-5239.1; SECNAV 5239.3B; MCO 5239.2A, ECSD 020
405 07	CONTINGENCY AND CONTINUITY OF OPERATIONS PLANNING
405 07 001	Does the command have a Continuation of Operations Plan (COOP) that properly identify mission and business essential functions for the priority restoration of all assets supporting the mission and business essential functions (e.g., computer-based services, data and applications,

communications, physical infrastructure)?
Reference
DODD 3020.26; CJCSI 6510.01F; SECNAV M-5239.1; SECNAV 3030.4C; SECNAV 3501.1B; MCO 3030.1

405 07 002 Are the storage of backup files isolated from any network and physically separated from the originating facility?
Reference
NIST SP 800-34; CJCSI 6510.01F; MCO 5239.2A

405 07 003 Has an alternate site been identified that permits the full (MAC I or II) or partial (MAC III) restoration of mission or business essential functions, ensuring the enclave boundary defense at the alternate site provides security measures equivalent (MAC II and III) and configured identically (MAC I) to the primary site?
Reference
CJCSI 6510.01F; DODD 3020.26; SECNAV M-5239.1

405 07 004 Has the IT Contingency/Continuity Plan (COOP), to include deployed locations when a system is deployed, gone through Tabletop or Functional Exercises with proper documentation, lessons learned, and reporting requirements?
Reference
CJCSI 6510.01F; DODD 3020.26; SECNAV M-5239.1; MCO 3030.1

405 07 005 Is the backup copy of the current and comprehensive baseline inventory of all software, OS and hardware stored in a fire-rated container or otherwise not collocated with the original?
Reference
CNSSP No. 17; CJCSI 6510.01F; SECNAV 3030.4C

405 07 006 Are electrical systems configured to allow continuous or uninterrupted power to key IT assets?
Reference
CJCSI 6211.02C; SECNAV 3030.4C; MCO 3030.1

405 07 007 Have plans been developed for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action to minimize the risk of it being compromise?
Reference
CJCSI 6211.02C; DoD 5200.01, Volume 3

405 08 SOFTWARE/HARDWARE MANAGEMENT

405 08 001 Is the latest version of Anti-virus/HIPS software used with updated signatures on wireless-capable PED’s and workstations that are used to synchronize/transmit data?
Reference

	CJCSI 6510.01F; DODD 8100.02; DODI 8420.01; SECNAV M-5239.1
405 08 002	Are all IA or IA-enabled IT hardware, firmware, and software components or products in compliance with evaluation and validation requirements? Reference CJCSI 6510.01F; DODD 8500.01; DODI 8420.01; SECNAV M-5239.1; SECNAV 5239.3B
405 08 003	Are the purchase and implementation of Data At Rest (DAR) encryption technologies facilitated and implemented IAW the MCEN solution and with MCNOSC oversight? Reference DOD POLICY MEMO DTD 03 JUL 07; ERP V1R1.1 STIG, SEC 3.10.1, ERP 008300; MARADMIN 461/09; MARADMIN 639/09
405 08 004	Has all software used on IS's been purchased and/or licensed in accordance with established copyright laws and license provisions? Reference PUBLIC LAW 102-561; TRADITIONAL CHECKLIST STIG; MCO 5239.2A
405 08 005	Are all IT procurement requests, regardless of costs, processed and reviewed using the IT Procurement Request Approval System (ITPRAS)? Reference MARADMIN 298/08; MARADMIN 375/11
405 08 006	Are all IS's properly registered in the DoD IT Portfolio Registry (DITPR- DON)? Reference CJCSI 6211.02D; SECNAV 5239.3B
405 09	WIRELESS/PED'S
405 09 001	Are wireless technologies used for storing, processing, and/or transmitting unclassified information in areas where CLASSIFIED information is discussed, stored, processed, or transmitted without express written consent of the Marine Corps DAA and the Service Certified TEMPEST Technical Authority (CTTA)? Reference CJCSI 6510.01F; DODD 8100.02; SECNAV 2075.1; ECSD 005; ECSD 014
405 09 002	Does the SSID/ESSID contain any identifying information about the organization common phrases that may be associated with the Marine Corps, or product identifier? Reference NSA I332-008R-2005; NIST SP 800-48; ECSD 014

405 09 003 Are periodic assessments completed on UNCLASSIFIED wireless networks or does the UNCLASSIFIED and CLASSIFIED wired and wireless networks have Wireless Intrusion Detection (WIDS) capabilities to monitor WLAN activity and identify WLAN related policy violations?
Reference
CJCSI 6510.01F; NSA I332-008R-2005; DODI 8420.01; SECNAV 2075.1

405 09 004 Are all government PED that have been assigned throughout the command to individual being properly tracked as part of the organizational inventory?
Reference
CJCSI 6510.01F; ECSD 005; ECSD 014

405 09 005 Have all personnel with access to Government issued PEDs signed and accepted the terms of the PED Rules of Behavior document prior to use?
Reference
CJCSI 6510.01F; ECSD 005; ECSD 014

405 09 006 Are all PEDs capable of supporting digital signature and encryption (Secure/Multipurpose Mail Extensions (S/MIME)) functionality able to interface with PKI certificates stored on DoD-approved hardware tokens including the Common Access Card (CAC)?
Reference
DODI 8520.2; DON CIO MESSAGE DTG: 202041Z; MARADMIN 659/08; MARADMIN 649/09; ECSD 005

405 09 007 Are wireless peripherals operating on radio-frequency (RF) or 802.15 WPAN (Bluetooth, IrDA, UWB, Z-Wave, or ZigBee) technologies or are IR peripherals permitted to transfer between CLASSIFIED and UNCLASSIFIED environments?
Reference
CNSSP NO. 17, SEC.IV, PAR 5.A.X; DODD 8100.2; ECSD 014

405 10 REMOTE ACCESS/VPN'S

405 10 001 Are signed user agreements completed by all remote users prior to obtaining access?
Reference
REMOTE ACCESS POLICY STIG V2R1; ECSD 014

405 10 002 Are all remote connections identified, authenticated, and logged?
Reference
SECNAV 5239.3B; ECSD 014